

**REMARKS**

This Preliminary Amendment is filed concurrently with a Reissue Application for U.S. Patent No. 5,848,159 (hereafter the "original patent").

**Status of the Claims:**

As of the date of this Preliminary Amendment, claims 1-13 of the original patent are amended and remain pending; claims 14-61 have been added. Thus, claims 1-61 are now pending in the Reissue Application.

**Statement of Support in the Disclosure of the Original Patent for the Amendments:****The Specification:**

The specification of the original patent has been amended to correct typographical errors and other matters of form and to render the specification consistent throughout and with the claims. Support for the amendments to the specification may be found throughout the original patent. No new matter has been introduced by the amendments to the specification.

In general, changes embodying corrections of typographical errors and other matters of form are self explanatory and need no further explanation. As to the mathematical expressions, equations expressing any congruence of the form  $b=c(\text{mod } m)$  or the like, where  $b$  is congruent to  $c$  and  $m$  is the modulus, are mathematically written in proper form as  $b\equiv c(\text{mod } m)$ . Accordingly all the equations are written in proper form, e.g.,  $C\equiv M^e(\text{mod } n)$ . Where applicable, the parentheses (e.g., around "mod  $n$ ") are properly added as well.

Support for amendments to the paragraph beginning at column (hereafter "col."), line 4 may be found in col. 1 of the cover page. Support for the amendments to the paragraph beginning at col. 3, line 23 and the paragraph beginning at col. 3, line 27 may be found for example at col. 2 of the cover page and col. 13, lines 44-47.

Support for amendments to the paragraph beginning at col. 3, line 36, may be found at column 5, lines 31-33. Support for amendments to the paragraph beginning at col. 3, line 56, may be found for example at col. 3, lines 20-26, col. 3, lines 44-55 and col. 4, lines 9-11. Support for amendments to the paragraph beginning at col. 4, line 6, may be found for example at col. 3, lines 20-26, col. 4, lines 6-12, 32-34 and 52-56.

Support for amendments to the paragraph beginning at col. 4, line 13 and the paragraph beginning at col. 4, line 50, may be found for example at col. 3 line 42, col. 4, line 41, and col. 10, lines 54-56. Further support for amendments to the paragraph beginning at col. 4, line 50 may be found at col. 4, lines 50-52.

Support for paragraph inserted before the paragraph beginning at col. 5, line 52, may be found for example at col. 14, lines 30-36 and 45-49. Support for amendments to the paragraph beginning at col. 5, line 30, may be found for example at col. 2, lines 5-10, col. 3, line 42, col. 4 line 41, col. 5, line 39, col. 10, line 65 and col. 11, lines 8-9. Further support for amendments to the paragraph beginning at col. 5, line 30, may be found in the multitude of mathematical expressions where  $d$ , the private key portion, is the "exponent," e.g.,  $M \equiv C^d \pmod{n}$  at col. 6, lines 1-5.

Support for amendments to the paragraph beginning at col. 6, line 24, may be found for example at col. 5, lines 31-33, col. 6, line 37 (" $M=Y_k...$ "), col. 7, line 15, and col. 11, lines 15-20. Support for amendments to the paragraph beginning at col. 6, line 65, may be found for example at col. 6, lines 1-4, 26-35, 40-53 and 67. Support for amendments to the paragraph beginning at col. 7, line 1, may be found for example at col. 2, lines 32-34 and 40, col. 3, lines 22-26, col. 4, lines 32-34, col. 6 line 38 and col. 7, lines 56-58.

Support for amendments to the paragraph beginning at col. 8, line 1, is found in col. 8 line 3 (i.e., FIPS 140-1 with level 3 is a well known standard, See: <http://csrc.nist.gov/fips/fips1401.htm>). Support for amendments to the paragraph beginning at col. 10, line 15, may be found for example at Figure 3. Support for amendments to the paragraph beginning at col. 10, line 35, may be found for example in col. 10 line 40 and line 53 (i.e.,  $M$  is represented by a numerical value greater than 0 and smaller than  $n$ ).

### The Claims:

Claims 1-13 of the original patent have been amended to correct typographical errors and other matters of form, as well as to recite more clearly and particularly the subject matter which Applicants regard as their invention. New claims 14-61 have been added to further point out and distinctly claim subject matter which Applicants regard as their invention. Support for the amendments to claims 1-13 and for the newly added claims, 14-61, may be found throughout the original patent. No new matter has been introduced by the amendments to the claims.

In general, claim amendments embodying corrections of typographical errors, antecedent basis errors, and other matters of form are self explanatory and need no further explanation. As to the mathematical expressions, equations expressing any congruence of the form  $b \equiv c \pmod{m}$  or the like, where  $b$  is congruent to  $c$  and  $m$  is the modulus, are mathematically written in proper form as  $b \equiv c \pmod{m}$ . Accordingly all the equations are written in proper form, e.g.,  $C \equiv M^e \pmod{n}$ . Where applicable, parentheses (e.g., around “mod  $n$ ”) are properly added as well.

Support for amendments to claim 1 as now presented may be found, for example, at claim 1 as presented in the original patent, as well as col.1, lines 32-42, col. 3, lines 39-44, col. 5, lines 30-33, col. 7, lines 25-28 and col. 8, lines 8-11. Support for amendments to claim 2 as now presented may be found, for example, at claims 1 and 2 as presented in the original patent, as well as col. 2, lines 24-30, col. 5, lines 36-40 and col. 14, lines 19-24. Similarly, support for amendments to claims 3-13 as now presented may be found, for example, at claims 1-13 as presented in the original patent. Further support for the amendments to claims 3-13 as now presented may be found for example at col.1, lines 32-42, col. 2, lines 24-30, col. 3, lines 39-44, col. 5, lines 30-40, col. 7, lines 25-28, col. 8, lines 8-11, and col. 14, lines 19-24. Further support for amendments to claim 12 as now presented may be found for example at col.9, lines 48-50.

As to the newly added claims, support for claim 14-23, 40-43, and 50-58 may be found, for example, at col. 1, lines 32-42, col.3, lines 35-44, col. 4, lines 37-49, col. 5, lines 30-33 and 36-51, col. 7, lines 25-28, col. 8, lines 8-11, col. 14, lines 30-36. Further support for new claims 14-23, 40-43, and 50-58 may be found at claims 1-13 as presented in the original patent. For example, support for new claims 18 and 19 may be found in claim 9, i.e., col. 14, lines 30-36. Further support for new claims 20 and 22 may be found at col. 3, lines 30-36 and 53-55, and col. 7, lines 25-28. Support for new claims 24-33 may be found for example at column 3, lines 36-65.

Support for new claims 34-39 may be found for example at col. 4, lines 8-12 and col. 5, lines 61-63. Further support for new claims 40 and 41 may be found at col. 5, lines 58-61. Further support for new claims 42, 43, 50-52, and support for new claims 44-49 may be found at Figures 1-3, and the accompanying description at col. 7, line 34 to col. 10, lines 34. Further support for new claims 50-54 may be found at col. 5, line 52 to col. 6, line 6. Finally, support for claims 60 and 61 may be found at col. 4, lines 6-13 and col. 5, lines 61-63.

**Summary:**

Entry of the foregoing amendments to the specification and claims is hereby respectfully requested. Claims 1-61 are now presented for examination in the Reissue Application which is believed to be in condition for allowance. Prompt examination and allowance of the pending claims is therefore respectfully requested.

**Concurrent Office Proceedings; and Petition for Waiver of Delay:**

It is noted that Reexamination Requests respecting the original patent have been filed with the U.S. Patent and Trademark Office on May 18, 2000 (Order Granting Reexamination mailed July 19, 2000; Control No. 90/005,733) and on July 28, 2000, respectively. In view of the concurrent office proceedings, Reexamination and Reissue Application, it is hereby requested that the Reexamination proceeding be stayed until the Reissue Application proceeding is concluded, or, in the alternative, that the Reexamination proceeding be merged with the Reissue Application proceeding (37 C.F.R. 1.565(d)).

In view of the concurrent office proceedings, a Petition under 37 C.F.R. 1.183 to waive the 2-months delay for protest is attached herewith. Examination of the Reissue Application should commence without delay and before the Reexamination proceeds.


**Fee Authorization:**

If for any reason an insufficient fee has been paid, the Commissioner is hereby authorized to charge any deficiency in payment of required fees associated with this communication to Deposit Account **02-3964**.

Date: October 19, 2000

Respectfully submitted,

Oppenheimer Wolff & Donnelly LLP  
3373 Hillview Avenue  
Palo Alto, CA 94304  
Tel: (650) 320-4000

  
By: Leah Sherry,  
Attorney for Applicant  
Reg. No. 43,918

JC914 U.S. PRO  
09/694416  
10/20/00

**CERTIFICATE OF MAILING (37 CFR 1.10(a))**

CERTIFICATE OF MAILING BY "EXPRESS MAIL" - Rule 10: I hereby certify that this correspondence is being deposited on October 5, 2000 with the U.S. Postal Service "Express Mail Post Office to Addressee" under 37 CFR 1.10 as **Express Mail No. EL655031318US** addressed to: Box Reissue Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231

Date: October 19, 2000

